#20/E
BH
6-24-01

UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: COLLINS et al. Atty Docket No: 20206-25 (PT-TA 410 (Cont 1))
Serial No: 09/328,726 Group Art Unit: 2131
Filing Date: October 26, 1998 Examiner: Leaning, J.
For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Box No Fee Amendment
Assistant Commissioner for Patents
Washington, D.C. 20231

AMENDMENT

Sir:

In response to the Office Action mailed on April 2, 2001, Applicants respectfully request reconsideration of the above-identified patent application. Please amend the above identified application as follows and consider the following remarks.

In The Claims:

14. (Three Times Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key transformation schemes, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, where M corresponds to a number representative of a message and

$0 \leq M \leq n-1$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ where k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, and where the ciphertext word C is a number representative of an encoded form of message word M, said encoding step including the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

$$\vdots$$